REMARKS

A. INTRODUCTION

In the final Office Action mailed on October 5, 2006, the Examiner rejected claims 30-33, 35, 38-41, 43, and 46-49 under 35 U.S.C. § 103(a) over U.S. Patent No. 6,691,232 to Wood, et al. ("Wood") and U.S. Patent No. 6,728,884 to Lim; and rejected claims 34, 36-37, 42, 44-45, and 50 under 35 U.S.C. § 103(a) over Wood, Lim, and Applicant Admitted Prior Art (AAPA).

Claims 30-50 are pending in this application. In this response, applicant amends claims 30, 38, and 46 to clarify the subject matter for which applicant seeks protection. No new matter is added. For the reasons discussed in detail below, applicant submits that the pending claims are now all in condition for allowance.

B. DISCUSSION OF INTERVIEW

Applicant would like to thank the Examiner for her consideration during the telephone interview of December 7, 2006. During the interview, the Examiner and applicant's representative discussed the Section 103(a) rejection of the claims based primarily on Wood. The Examiner and applicant's representative agreed that applicant's primary argument is that the order of events that occur under applicant's techniques differs from that of Wood.

The Examiner's primary concern is that the claims do not adequately distinguish certain embodiments of Wood. In particular, the Examiner pointed out that in some embodiments of Wood an authentication methodology is determined before an entity requests access to a resource of a server, similar to applicant's techniques. (Wood, 11:23-28.) In these embodiments, Wood describes an entity that initially requests access to a login page, but does not request access to a particular resource. After the entity requests access to the login page, the server provides the entity with a list of possible authentication methodologies that are adequate for the lowest trust level. This is appropriate, as the entity has not yet requested a resource with which a particular level of trust is associated. The entity selects an authentication methodology and provides the server with one or more

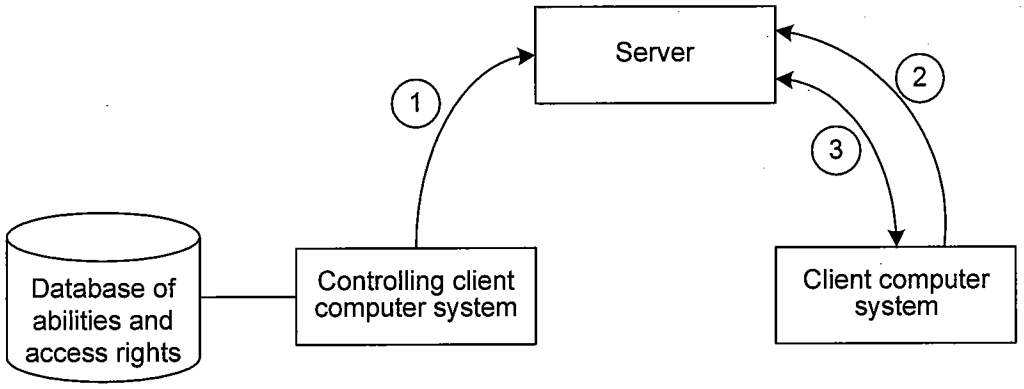
credentials as necessary for authentication under the selected authentication methodology. (Wood, 11:34-38.) The server then authenticates the entity according to the selected authentication methodology. (Wood, 12:13-15.) If the server can authenticate the entity, access to the login page will be granted. (Wood, 9:40-43.) Once the entity has been granted access to the login page, the entity may subsequently request access to a particular resource of the server. If the entity has a sufficient trust level for access to the resource (i.e., the resource requires only the lowest trust level), access to the resource is granted. (Wood, 2:41-46.) If the entity does not have a sufficient trust level, it may obtain a credential upgrade. (Wood, 2:46-48.) The server will provide the entity with a list of possible authentication methodologies that are adequate for the sufficient trust level. The entity will select an authentication methodology and provide one or more credentials as necessary for authentication under the selected authentication methodology. (Wood, 11:34-38.) The server then authenticates the entity according to the selected methodology. (Wood, 12:13-15.) In sum, when an entity requests initial access to a login page only, an authentication methodology is selected before an entity requests access to a resource of the server. Authentication of the entity also occurs before the entity's request. If an entity later requests access to a resource for which the entity has not obtained a sufficient trust level, an adequate authentication methodology may be selected and an entity may be re-authenticated.

Applicant has amended independent claims 30, 38, and 46 to recite that a request from a client computer system to access a service of the server computer is received "before authenticating the client computer system" and that the authentication that occurs after the request from the client computer system is received is the "initial[]" authentication (i.e., it is the first time the client computer system has been authenticated).

In contrast to Wood, applicant's amended claims thus recite that the request to access a resource is received before the client computer system is authenticated. The embodiments of Wood just described disclose that the request to access a resource is received after the client computer system is authenticated. In addition, applicant's amended claims recite that the authentication that occurs after the client request is the

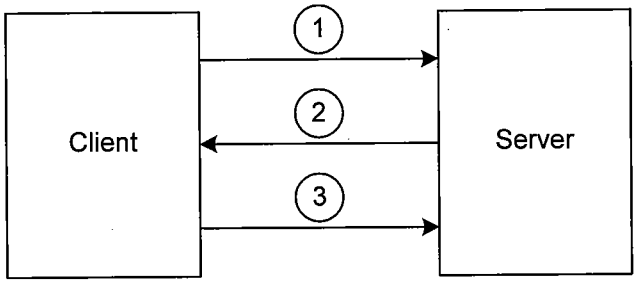
initial authentication (i.e., the first time the client is authenticated). In contrast, the embodiments of Wood just described disclose that the authentication that occurs after the client request is a re-authentication (i.e., the client has previously been authenticated, at a lower trust level). Accordingly, applicant respectfully submits that the amended claims are clearly patentable over Wood.

C. APPLICANT'S TECHNIQUES



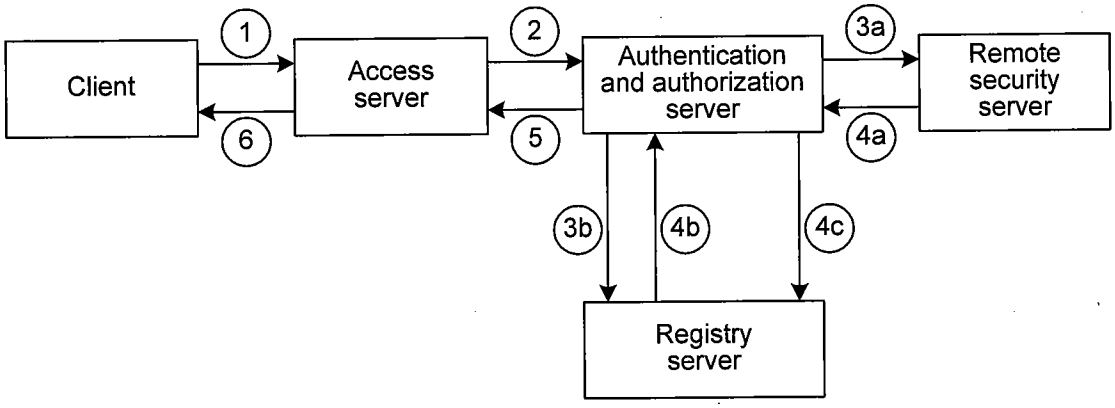
Applicant's techniques are directed to determining an authentication methodology prior to a client requesting access to a server. A controlling client computer system provides (1) an instruction to a server. The instruction indicates an authentication methodology that is to be used to authenticate a client computer system. After the server has received this instruction from the controlling client computer system, the server may receive (2) an access request from the client computer system. After receiving an access request from the client computer system, the server authenticates (3) the client computer system using the authentication methodology indicated by the instruction received from the controlling client computer system.

D. WOOD



Unlike applicant's techniques, Wood describes a client requesting (1) access to a server's applications and/or resources prior to determination of an authentication methodology (col. 7, lines 34-40). After a client has requested access to the server, the server, via a login component, provides (2) the client with a list of suitable authentication schemes, from which the client may select (col. 11, lines 34-38). The client then selects (3) an authentication scheme and the server authenticates the client using the selected scheme.

E. LIM



Unlike applicant's techniques, Lim also describes a client requesting (1) access to a server prior to determination of an authentication methodology (col. 5, lines 18-23, 30-31, 45-49). After the client has requested access to the server, the access server requests (2) authentication of the client from the authentication and authorization server. The access server may transmit to the authentication and authorization server any authentication information received from the client, including user id, password, and a list of the remote

security servers that can authenticate the user (col. 5, lines 63-67). The authentication and authorization server initially authenticates (3a) the client through use of the remote security server. Data received from a remote security server is stored (4c) in the registry server for later use (3b) by the authentication and authorization server for subsequent authentication of the client without having to use the remote security server. The remote security server manages authentication profiles of clients and may authenticate a user based on the user id and password supplied by the client (col. 4, lines 31-32). The registry server is a central repository that contains authentication profiles of clients, including user id and password (col. 6, lines 11-19). Once it receives (4a and 4b) a result from either the remote security server or the registry server, the authentication and authorization server returns (5) information to the access server that indicates whether the client is authorized and what are its access rights (col.5, line 67 – col. 6, line 3). Data representing the client's access rights is stored (6) in a cookie in the client's browser.

F. PRIOR ART REJECTIONS

Claims 30-50 stand rejected over Wood and Lim alone or in combination with AAPA, under 35 U.S.C. § 103(a). Applicant respectfully traverses this rejection.

All of the claims are directed to a server being provided with an instruction from a controlling client computer system (or controlling entity) prior to the server receiving a request from a client computer system (or client entity) to access a service of the server. In addition, all of the claims are directed to the instruction indicating an authentication methodology, the authentication methodology being selected from multiple authentication methodologies. Claims 30-37 recite:

> A method in a server computer of authenticating client computer systems, the method comprising:
>
> receiving from a controlling client computer system an instruction that indicates an authentication methodology that is to be used to authenticate a client computer system ..., the authentication methodology being selected from multiple authentication methodologies ...;

> after receiving the instruction, receiving a request from the client computer system to access a service of the server computer system; ...

Claims 38-45 recite:

> A method in a controlling client computer system for providing indications of authentication methodologies to a server computer system, the method comprising:
>
> generating an instruction that indicates an authentication methodology that is to be used to authenticate a client computer system ..., the authentication methodology being selected from multiple authentication methodologies ...; and
>
> sending the generated instruction to the server computer system so that upon receiving a request from the client computer system to access a service of the server computer system after the instruction is received at the server computer system ....

Claims 46-50 recite:

> A tangible computer-readable medium containing instructions for controlling a server computer system to authenticate entities, by a method comprising:
>
> receiving from a controlling entity an instruction that indicates an authentication methodology that is to be used to authenticate an entity, the authentication methodology being selected from multiple authentication methodologies ...;
>
> after receiving the instruction from the controlling entity, receiving a request from the entity to access a service of the server computer system; ...

Neither Wood nor Lim teaches or suggests a server being provided with an instruction from a controlling client computer system (or controlling entity) prior to the server receiving a request from a client computer system (or client entity) to access a service of the server. In contrast, Wood and Lim both describe a client first requesting access to a server (Wood, col. 7, lines 34-40; Lim, col. 5, lines 18-23, 30-31, 45-49). The Examiner believes that Wood does not require a client to first request access to a server. The Examiner stated:

> Wood did not explicitly disclose the access request is received after the authentication instruction, however, Wood does state it is not necessary for

> the user to request access before determining suitable authentication methods (see col 11 lines 23-29). This implies the claimed order because requesting access to a resource is necessary before accessing the resource.

Wood does describe a situation in which a user does not request access to any particular information resource:

> If there is no particular resource for which access is being requested (e.g., if a user jumps straight to a sign-on page without requesting an access), the service will proceed according to the lowest level of trust available consistent with session environment.

(col. 11, lines 23-28, emphasis added). However, in such a case, the user is still requesting access to the "service" of the server. Wood defines access as "presenting a URL to gatekeeper/entry handler component, which acts as a point of entry for client entities requesting applications and/or resources controlled by the security architecture" (col. 7, lines 34-40). When the client submits the URL of the sign-on page, it is requesting access to the service of the server, even if not to a particular information resource. Because the client has not yet requested an information resource, for which there is an associated trust level, the server may proceed to its service according to the lowest level of trust (col. 11, lines 23-29). Further, under Wood the authentication methodology cannot be chosen prior to a client requesting access, because the client must select an authentication methodology from a list of suitable methodologies provided to it by the server (via the login component) (col. 11, lines 34-51). This must necessarily occur after a client has requested access to the server, establishing communication with the server. Thus, Wood does not teach or suggest after receiving an instruction that indicates the authentication methodology, receiving or sending "a request ... to access a service."

Like Wood, but unlike applicant's techniques, Lim describes a user first requesting access to a server (col. 5, lines 18-23, 30-31, 45-49). In addition, Lim does not disclose selecting an authentication methodology from multiple authentication methodologies based on the abilities and access rights of the client. Lim describes use of only *one* authentication methodology, one that is based on user id and password. The Examiner stated that "Lim disclosed a Registry Server containing information on how a user should be authenticated." However, this information is simply an authentication profile that may

include user id, password, and a list of the remote security servers that can authenticate the user (col.6, lines 12-19). Lim uses the user id and password provided by a client to determine, using a single authentication methodology (whether via a remote security server or the registry server), the access rights had by the user. Lim describes access rights that are established as a result of the authentication process, in contrast to applicant's techniques, which are directed to a client's access rights assisting in determining the authentication methodology selected. Thus, Lim does not teach or suggest selecting an authentication methodology from multiple authentication methodologies based on the abilities and access rights of the client; nor does Lim teach or suggest after receiving an instruction that indicates the authentication methodology, receiving or sending "a request ... to access a service."

Based on the foregoing, all of the claims are patentable.

G. CONCLUSION

In view of the above remarks, applicant believes the pending application is in condition for allowance and respectfully requests reconsideration. If the Examiner has any questions or believes a telephone conference would further expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-8548.

Dated: 1-5-07

Respectfully submitted,

By Maurice J. Pirio

Maurice J. Pirio
Registration No.: 33,273
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8548
(206) 359-9548 (Fax)
Attorney for Applicant